Calendar No. 883

99TH CONGRESS, 2d Session | SENATE | REPORT 99-432

COMPUTER FRAUD AND ABUSE ACT OF 1986

SEPTEMBER 3, 1986.—Ordered to be printed

Filed under authority of the order of the Senate of August 16 (legislative day, August 11), 1986

Mr. THURMOND, from the Committee on the Judiciary, submitted the following

REPORT

together with

ADDITIONAL VIEWS

[To accompany S. 2281, as amended]

The Committee on the Judiciary, to which was referred the bill (S. 2281) to amend title 18, United States Code, to provide additional penalties for fraud and related activities in connection with access devices and computers, and for other purposes, having considered the same, reports favorably thereon with amendments and recommends that the bill, as amended, do pass.

CONTENTS

I. GENERAL STATEMENT AND HISTORY OF THE LEGISLATION

During the past several years, the Congress has been investigating the problems of computer fraud and abuse to determine wheth-

63-281 O

er Federal criminal laws should be revised to cope more effectively with such acts. The Judiciary Committee's concern about these problems has become more pronounced as computers proliferate in businesses and homes across the nation and as evidence mounts that existing criminal laws are insufficient to address the problem of computer crime.

For some time, the United States has been in the midst of a technological explosion. The Federal Government alone operates more than 18,000 medium-scale and large-scale computers at some 4,500 different sites, and the Office of Technology Assessment estimates the Government's investment in computers over the past four years at roughly $60 billion. The General Services Administration estimates that there will be 250,000 to 500,000 computers in use by the Federal Government by 1990.

Computer use has also become much more widespread among the nation's private sector. In 1978, there were an estimated 5,000 desk-top computers in this country; today there are nearly 5 million. Financial institutions, in particular, rely heavily on computer communications; for instance, the Bureau of Justice Statistics reported that in 1983, corporate transfers of funds via computer totaled more than $100 trillion.[1] In addition, more than 100,000 personal computers have been installed in the country's schools, and computers are found in millions of American homes.

This technological explosion has made the computer a mainstay of our communications system, and it has brought a great many benefits to the government, to American businesses, and to all of our lives. But it has also created a new type of criminal—one who uses computers to steal, to defraud, and to abuse the property of others. The proliferation of computers and computer data has spread before the nation's criminals a vast array of property that, in many cases, is wholly unprotected against crime.

In June 1984, the American Bar Association Task Force on Computer Crime, chaired by Joseph Tompkins, Jr., issued its Report on Computer Crime (hereinafter referred to as the "ABA Report"), a study based upon a survey of approximately 1,000 private organizations and public agencies.[2] The ABA Report found that more than 50 percent of the 283 respondents had been victimized by some form of computer crime,[3] and that more than 25 percent of the respondents had sustained financial losses totaling between an estimated $145 million and $730 million during one twelve-month period.[4] The ABA Report also concluded that computer crime is among the worst white-collar offenses.[5] The Committee agrees but notes particularly that computer crimes pose a threat that is not solely financial in nature.

In 1983, for example, a group of adolescents known as the "414 Gang" broke into the computer system at Memorial Sloan-Kettering Cancer Center in New York. In so doing, they gained access to

[1] Bureau of Justice Statistics, *Report on Electronic Funds Transfer Fraud,* March 1985, NCJ-96666.
[2] *Report on Computer Crime;* Task Force on Computer Crime, Section of Criminal Justice, American Bar Association; June 1984)
[3] Ibid., pp. 16–18, Table 12.
[4] Ibid., p. 38.
[5] Ibid., pp. 36–40.

the radiation treatment records of 6,000 past and present cancer patients and had at their fingertips the ability to alter the radiation treatment levels that each patient received. No financial losses were at stake in this case, but the potentially life-threatening nature of such mischief is a source of serious concern to the Committee.

Similarly, so-called "pirate bulletin boards" have sprung up around the country for the sole purpose of exchanging passwords to other people's computer systems. The *Richmond (Va.) Times-Dispatch* recently reported that three such bulletin boards operating in Virginia carry information on how to break into the computers of the U.S. Defense Department and the Republican National Committee. While financial losses resulting from such pirate bulletin boards may not be imminent, the Committee believes that knowingly trafficking in other people's computer passwords should be proscribed.

It is clear that much computer crime can be prevented by those who are potential targets of such conduct. The ABA Report indicated that while the respondents to the survey overwhelmingly supported a Federal computer crime statute,[6] they also believed that the most effective means of preventing and deterring computer crime is "more comprehensive and effective self-protection by private business" [7] and that the primary responsibility for controlling the incidence of computer crime falls upon private industry and individual users, rather than on the Federal, State, or local governments.[8] The Committee strongly agrees with these views.

The Committee also finds that education programs for both computer users and the general public should be undertaken to make young people and others aware of the ethical and legal questions at stake in the use of computers and to deflate the myth that computer crimes are glamorous, harmless pranks. The respondents to the ABA survey indicated strong support for such programs,[9] many of which are underway throughout the nation. The Committee commends those education and security improvement efforts and urges their continuation.

At the same time, the Committee finds that Federal criminal penalties for computer crime are an appropriate punishment for certain acts and can serve to deter would-be computer criminals and to reinforce education and security improvement programs.

To that end, both the Senate and House have devoted considerable attention to determining how the Federal Government can best approach computer-related crimes. The first Federal computer crime statute was enacted in 1984 as part of P.L. 98-473. This is the present 18 U.S.C. 1030, which makes it a felony to access classified information in a computer without authorization and makes it a misdemeanor to access financial records or credit histories in financial institutions or to trespass into a Government computer.

Legislation was introduced in both the Senate and House early in the 99th Congress to expand and to amend 18 U.S.C. 1030. On

[6] Ibid., p. 44.
[7] Ibid., p. 23, Table 17.
[8] Ibid., p. 11, Table 8.
[9] Ibid., p. 23, Table 17.

May 23, 1985, the House Subcommittee on Crime held a hearing on H.R. 1001 (introduced by Representative William J. Hughes (D-N.J.) and H.R. 930 (introduced by Representative Bill Nelson (D-Fla.). Representative Bill McCollum, R-Fla., subsequently introduced a computer crime bill, H.R. 3381, at the request of the Department of Justice. The Senate Subcommittee on Criminal Law held a hearing on October 30, 1985, on two computer crime bills: S. 440 (introduced by Senator Paul Trible (R-Va.) and S. 1678 (introduced by Senator Strom Thurmond, (R-S.C., at the request of the Department of Justice). S. 1678 is the Senate companion to H.R. 3381.

As a result of the testimony given at both the Senate and House hearings, Senator Trible and Representative Hughes introduced identical computer crime bills (S. 2281 and H.R. 4562) on April 10, 1986. The House Subcommittee on Crime considered H.R. 4562 on April 23, and on April 30 the subcommittee forwarded a clean bill, H.R. 4718, to the Committee on the Judiciary in lieu of H.R. 4562. The Committee on the Judiciary ordered H.R. 4718, as amended, reported on May 6 (see House Report 99-612), and on June 3 the House passed the bill by voice vote. In the Senate, the Committee on the Judiciary held a hearing on S. 2281 on April 16, 1986. The Committee ordered the bill, as amended, reported to the Senate on June 12, 1986.

Throughout its consideration of computer crime, the Committee has been especially concerned about the appropriate scope of Federal jurisdiction in this area. It has been suggested that, because some States lack comprehensive computer crime statutes of their own, the Congress should enact as sweeping a Federal statute as possible so that no computer crime is potentially uncovered. The Committee rejects this approach and prefers instead to limit Federal jurisdiction over computer crime to those cases in which there is a compelling Federal interest, i.e., where computers of the Federal Government or certain financial institutions are involved, or where the crime itself is interstate in nature. The Committee is convinced that this approach strikes the appropriate balance between the Federal Government's interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses.

S. 2281, as reported by the Committee, is a consensus bill aimed at deterring and punishing certain "high-tech" crimes in a manner consistent with the States' own criminal laws in this area.

II. Discussion of Committee Action and Amendments

On June 12, 1986, the Committee on the Judiciary met and unanimously ordered S. 2281 reported favorably to the full Senate. Several minor amendments were also approved unanimously by the Committee.

The first amendment was a technical change to page two, line eight of the bill, made necessary because of the second Committee amendment. That second amendment struck lines 9-24, relating to unauthorized access of Government computers, on page two, and inserted in their place the language that forms the new subsection 18 U.S.C. 1030(a)(3), as reported. That subsection is explained in detail in the section-by-section analysis of this Report.

The third Committee amendment struck the new subsection (a)(5) from S. 2281 as introduced, and replaced it with amended language. In so doing the Committee added to (a)(5) the words "damages, or destroys" to make explicit the subsection's application to acts—such as erasing data—that go beyond mere alteration of information. This amendment also changed "that computer" (as written in the original S. 2281) to "any such Federal interest computer". The Committee wanted to prevent the possibility that a defense would be raised to the effect that the information that was altered, damaged, or destroyed, was not in the very same computer on to which the offender had signed. The use of "any such Federal interest computer" makes clear that no such defense is possible. This amendment also deleted "another" from the portion of S. 2281 relating to subsection (a)(5); the phrase "one or more others" was inserted in its place. The Committee does not intend that every victim of acts proscribed under (a)(5) must individually suffer a loss of $1,000. Certain types of malicious mischief may cause smaller amounts of damage to numerous individuals, and thereby collectively create a loss of more than $1,000. By using "one or more others", the Committee intends to make clear that losses caused by the same act may be aggregated for purposes of meeting the $1,000 threshold. Finally, this amendment added to the coverage of the new subsection (a)(5) acts that alter, damage, or destroy computerized medical records, and thereby impair or threaten to impair an individual's medical care. The Committee's rationale for this addition is explained more fully in the section-by-section analysis pertaining to the new 18 U.S.C. 1030(a)(5).

The fourth Committee amendment changed "such use" to "the use of the financial institution's operation or the Government's operation of such computer". This change simply makes clear that a computer that is not used exclusively by the United States Government or by a financial institution, as that term is defined by proposed 18 U.S.C. 1030(e)(4), is a Federal interest computer only to the extent that its use by the Government or the financial institution is affected. This clarification also appears in the Committee's amendment affecting proposed 18 U.S.C. 1030(a)(3).

The fifth Committee amendment was merely a technical change made necessary because the sixth Committee amendment added "department of the United States" to the list of terms defined in the bill.

III. Section-by-Section Analysis

The following is a section-by-section analysis of S. 2281, as reported by the Committee on the Judiciary.

Section 1 of the bill contains its short title, the "Computer Fraud and Abuse Act of 1986".

Section 2(a)(1) amends 18 U.S.C. 1030(a)(2) to change the scienter requirement from "knowingly" to "intentionally", for two reasons. First, intentional acts of unauthorized access—rather than mistaken, inadvertent, or careless ones—are precisely what the Committee intends to proscribe. Second, the Committee is concerned that the "knowingly" standard in the existing statute might be inappropriate for cases involving computer technology. The Senate's

Report on the Criminal Code (Report No. 96-1396, pg. 33, citing *United States* v. *United States Gypsum Co.*, 438 U.S. 422, 425 (1978)), states that a person is "said to act knowingly if he is aware 'that the result is practically certain to follow from his conduct, whatever his desire may be as to that result.' " (Footnote omitted.) While appropriate to many criminal statutes, this standard might not be sufficient to preclude liability on the part of those who inadvertently "stumble into" someone else's computer file or computer data. This is particularly true in those cases where an individual is authorized to sign onto and use a particular computer, but subsequently exceeds his authorized access by mistakenly entering another computer file or data that happens to be accessible from the same terminal. Because the user had "knowingly" signed onto that terminal in the first place, the danger exists that he might incur liability for his mistaken access to another file. This is so because, while he may not have desired that result, i.e., the access of another file, it is possible that a trier of fact will infer that the user was "practically certain" such mistaken access could result from his initial decision to access the computer. The substitution of an "intentional" standard is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another. Again, this will comport with the Senate Report on the Criminal Code, which states that " 'intentional' means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective." (Footnote omitted.)

Section 2(a)(2) deletes from the existing 18 U.S.C. 1030(a)(2) the phrase "as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.),". The terms to which that phrase is applicable, "financial institution" and "financial record," are defined in section (2)(g) of S. 2281.

The premise of 18 U.S.C. 1030(a)(2) will remain the protection, for privacy reasons, of computerized credit records and computerized information relating to customers' relationships with financial institutions. This protection is imperative in light of the sensitive and personal financial information contained in such computer files. However, by referring to the Right to Financial Privacy Act, the current statute limits its coverage to financial institution customers who are individuals, or are partnerships with five or fewer partners. The Committee intends S. 2281 to extend the same privacy protections to the financial records of all customers—individual, partnership, or corporate—of financial institutions.

The Department of Justice has expressed concerns that the term "obtains information" in 18 U.S.C. 1030(a)(2) makes that subsection more than an unauthorized access offense, i.e., that it might require the prosecution to prove asportation of the data in question.[10] Because the premise of this subsection is privacy protection, the Committee wishes to make clear that "obtaining information" in this context includes mere observation of the data. Actual asportation, in the sense of physically removing the data from its origi-

[10] Statement of Victoria Toensing, Deputy Assistant Attorney General, Criminal Division; before the Senate Judiciary Committee, April 16, 1986.

nal location or transcribing the data, need not be proved in order to establish a violation of this subsection.

Section 2(b) of S. 2281 provides a substitute for the present 18 U.S.C. 1030(a)(3), and is designed to accomplish several goals.

First, it will change the scienter requirement from "knowingly" to "intentionally". The same explanation offered for section 2(a)(1) is applicable here.

Second, section 2(b) will clarify the present 18 U.S.C. 1030 (a)(3), making clear that it applies to acts of simple trespass against computers belonging to, or being used by or for, the Federal Government. The Department of Justice and others have expressed concerns about whether the present subsection covers acts of mere trespass, i.e., unauthorized access, or whether it requires a further showing that the information perused was "used, modified, destroyed, or disclosed." [11] To alleviate those concerns, the Committee wants to make clear that the new subsection will be a simple trespass offense, applicable to persons without authorized access to Federal computers.

The Committee wishes to be very precise about who may be prosecuted under the new subsection (a)(3). The Committee was concerned that a Federal computer crime statute not be so broad as to create a risk that government employees and others who are authorized to use a Federal Government computer would face prosecution for acts of computer access and use that, while technically wrong, should not rise to the level of criminal conduct. At the same time, the Committee was required to balance its concern for Federal employees and other authorized users against the legitimate need to protect Government computers against abuse by "outsiders." The Committee struck that balance in the following manner.

In the first place, the Committee has declined to criminalize acts in which the offending employee merely "exceeds authorized access" to computers in his own department ("department" is defined in section 2(g) of S. 2281). It is not difficult to envision an employee or other individual who, while authorized to use a particular computer in one department, briefly exceeds his authorized access and peruses data belonging to the department that he is not supposed to look at. This is especially true where the department in question lacks a clear method of delineating which individuals are authorized to access certain of its data. The Committee believes that administrative sanctions are more appropriate than criminal punishment in such a case. The Committee wishes to avoid the danger that every time an employee exceeds his authorized access to his department's computers—no matter how slightly—he could be prosecuted under this subsection. That danger will be prevented by not including "exceeds authorized access" as part of this subsection's offense.

In the second place, the Committee has distinguished between acts of unauthorized access that occur within a department and those that involve trespasses into computers belonging to another department. The former are not covered by subsection (a)(3); the latter are. Again, it is not difficult to envision an individual who,

[11] Ibid.

while authorized to use certain computers in one department, is not authorized to use them all. The danger existed that S. 2281, as originally introduced, might cover every employee who happens to sit down, within his department, at a computer terminal which he is not officially authorized to use. These acts can also be best handled by administrative sanctions, rather than by criminal punishment. To that end, the Committee has constructed its amended version of (a)(3) to prevent prosecution of those who, while authorized to use some computers in their department, use others for which they lack the proper authorization. By precluding liability in purely "insider" cases such as these, the Committee also seeks to alleviate concerns raised by Senators Mathias and Leahy that the existing statute casts a wide net over "whistleblowers," who disclose information they have gleaned from a government computer. Senators Mathias and Leahy first expressed their concerns in 1984 about the effect of the current statute on whistleblowers. Their concerns were embodied in S. 610, a bill they introduced early in the 99th Congress. (See, Statements by Senator Mathias and Senator Leahy, Congressional Record of March 7, 1985; pp. S 2728-2730. See also their "Additional Views" in this report.)

The Committee has thus limited 18 U.S.C. 1030(a)(3) to cases where the offender is completely outside the Government, and has no authority to access a computer of any agency or department of the United States, or where the offender's act of trespass is interdepartmental in nature. The Committee does not intend to preclude prosecution under this subsection if, for example, a Labor Department employee authorized to use Labor's computers accesses without authorization an FBI computer. An employee who uses his department's computer and, without authorization, forages into data belonging to another department, is engaged in conduct directly analagous to an "outsider" tampering with Government computers. In both cases, the user is wholly lacking in authority to access or use that department's computer. The Committee believes criminal prosecution should be available in such cases.

The Committee acknowledges that in rare circumstances this may leave serious cases of intradepartmental trespass free from criminal prosecution under (a)(3). However, the Committee notes that such serious acts may be subject to other criminal penalties if, for example, they violate trade secrets laws or 18 U.S.C. 1030 (a)(1), (a)(4), (a)(5), or (a)(6), as proposed in this legislation. The Committee believes this to be the best means of balancing the legitimate need to protect the Government's computers against the need to prevent unwarranted prosecutions of Federal employees and others authorized to use Federal computers.

The third goal of Section 2(b) is to clarify subsection (a)(3) to make clear that one trespassing in a computer used only part-time by the Federal Government need not be shown to have affected the operation of the government as a whole. The Department of Justice has expressed concerns that the present subsection's language could be construed to require a showing that the offender's conduct harmed the overall operation of the Government and that this would be an exceedingly difficult task for Federal prosecutors.[12]

[12] Ibid.

Accordingly, Section 2(b) will make clear that the offender's conduct need only affect the use of the Government's operation of the computer in question.

Section 2(c) substitutes the phrase "exceeds authorized access" for the more cumbersome phrase in present 18 U.S.C. 1030 (a)(1) and (a)(2), "or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend". The Committee intends this change to simplify the language in 18 U.S.C. 1030(a) (1) and (2), and the phrase "exceeds authorized access" is defined separately in Section (2)(g) of the bill.

Section (2)(d) adds three new offenses to 18 U.S.C. 1030. The new subsection 1030(a)(4) to be created by this bill is designed to penalize thefts of property via computer that occur as part of a scheme to defraud. It will require a showing that the use of the computer or computers in question was integral to the intended fraud and was not merely incidental. It has been suggested that the Committee approach all computer fraud in a manner that directly tracks the existing mail fraud and wire fraud statutes. However, the Committee was concerned that such an approach might permit prosecution under this subsection of acts that do not deserve classification as "computer fraud."

The Committee was concerned that computer usage that is wholly extraneous to an intended fraud might nevertheless be covered by this subsection if the subsection were patterned directly after the current mail fraud and wire fraud laws. If it were so patterned, the subsection might be construed as covering an individual who had devised a scheme or artifice to defraud solely because he used a computer to keep records or to add up his potential "take" from the crime. The Committee does not believe that a scheme or artifice to defraud should fall under the ambit of subsection (a)(4) merely because the offender signed onto a computer at some point near to the commission or execution of the fraud. While such a tenuous link might be covered under current law where the instrumentality used is the mails or the wires, the Committee does not consider that link sufficient with respect to computers. To be prosecuted under this subsection, the use of the computer must be more directly linked to the intended fraud. That is, it must be used by an offender without authorization or in excess of his authorization to obtain property of another, which property furthers the intended fraud. Likewise, this subsection may be triggered by conduct that can be shown to constitute an attempted offense.

This approach is designed, in part, to help distinguish between acts of theft via computer and acts of computer trespass. In intentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system. If that is all he obtains, the offense should properly be treated as a simple trespass. But because the offender has obtained the small bit of information needed to get into the computer system, the danger exists that his and every other computer trespass could be treated as a theft, punishable as a felony under this subsection. A similar problem arises from recommendations made to the Committee that every act of unauthorized access to a "Federal interest computer" be treated as theft of computer time,

punishable under this subsection as part of a scheme to defraud. The Committee agrees that the mere use of a computer or computer service has a value all its own. Mere trespasses onto someone else's computer system can cost the system provider a "port" or access channel that he might otherwise be making available for a fee to an authorized user. At the same time, the Committee believes it is important to distinguish clearly between acts of fraud under (a)(4), punishable as felonies, and acts of simple trespass, punishable in the first instance as misdemeanors. That distinction would be wiped out were the Committee to treat every trespass as an attempt to defraud a service provider of computer time. One simply cannot trespass into another's computer without occupying a portion of the time that that computer service is available. Thus, that suggested approach would treat every act of unauthorized entry to a Federal interest computer—no matter how brief—as an act of fraud, punishable at the felony level. The Committee does not believe this is a proper approach to this problem. For that reason, the Committee has excluded from coverage under this subsection those instances where "the object of the fraud and the thing obtained consists only of the use of the computer."

However, the Committee agrees that lost computer time resulting from repeated or sustained trespasses can reach a level of seriousness sufficient to warrant Federal prosecution. The Committee believes such instances are more appropriately punished under the provision of the new subsection (a)(5) relating to preventing authorized use of a computer. A more detailed explanation of the Committee's intent respecting lost computer time is contained in the analysis for (a)(5).

The Committee remains convinced that there must be a clear distinction between computer theft, punishable as a felony, and computer trespass, punishable in the first instance as a misdemeanor. The element in the new paragraph (a)(4), requiring a showing of an intent to defraud, is meant to preserve that distinction, as is the requirement that the property wrongfully obtained via computer furthers the intended fraud. The new felony created by this subsection limits its jurisdiction to "Federal interest computers." These are defined in Section (2)(g) of the bill as computers used by the Federal Government or by financial institutions, or as computers located in different States.

The scienter requirement for this subsection, "knowingly and with intent to defraud," is the same as the standard used for 18 U.S.C. 1029 relating to credit card fraud.

The new subsection 1030(a)(5) to be created by the bill is designed to penalize those who intentionally alter, damage, or destroy certain computerized data belonging to another. The "intentional" standard is the same as that employed in Section 2(a)(1) and 2(b)(1) of the bill. Like the new subsection 18 U.S.C. 1030(a)(3), this subsection will be aimed at "outsiders," i.e., those lacking authorization to access any Federal interest computer. It will penalize alteration, damage, or destruction in two circumstances. The first is those which cause a loss to the victim or victims totalling $1,000 or more in any single year period. The Committee believes this threshold is necessary to prevent the bringing of felony-level charges against every individual who modifies another's computer data. Some

modifications or alterations, while constituting "damage" in a sense, do not warrant felony-level punishment, particularly when almost no effort or expense is required to restore the affected data to its original condition. The $1,000 valuation has been reasonably calculated by the Committee to preclude felony punishment in those cases, while preserving the option of felony punishment in cases involving more serious alteration, damage, or destruction. In many instances where the requisite dollar amount cannot be shown, misdemeanor-level penalties will remain available against the offender under subsections 1030(a)(2) or 1030(a)(3).

The Department of Justice has suggested that the concept of "loss" embodied in this subsection not be limited to the costs of actual repairs. The Committee agrees and intends that other expenses accruing to the victim—such as lost computer time and the cost of reprogramming or restoring data to its original condition—be permitted to count toward the $1,000 valuation. The Committee wishes to leave no doubt that it intends lost computer time to be covered by this subsection. Once again, the Committee recognizes the inherent value of using computer time or of occupying a portion of the time that a computer service is made available. Many commercial services obtain revenue by charging authorized subscribers for the amount of time they are using the service. An unauthorized user can therefore impose substantial costs on the service provider by tying up one channel of access—a channel that the provider might otherwise be leasing at a profit to an authorized subscriber. The Committee recognizes this danger, and intends subsection (a)(5) to cover cases where an offender, having obtained unauthorized access to the computer, prevents authorized use of such a computer by occupying an access channel or "port" that is in demand by authorized subscribers. In the preceding discussion of subsection (a)(4), the Committee made clear that acts of trespass causing a loss of computer time should not be treated as acts of fraud for purposes of that subsection. However, it is clear that lost computer time can impose significant costs on providers of computer services. Where those costs total more than $1,000 in any one-year period, the Committee believes prosecution should be available under this subsection.

Likewise, the Committee intends that certain network communications costs be permitted to count toward the $1,000 valuation; a summary of a recent incident best illustrates this area. Often, a telecommunications firm (called the host company) will allow users from all over the country to access its computers by dialing a phone number that is local to the user. A second company (called a network company) will provide the service that connects the user, via phone lines, to the host company's computer, thus acting as a bridge between the two. The fee for the network company's service is often paid by the host company itself. In the incident under discussion, an unauthorized user programmed his computer to make repeated, automatic calls to the host company's computers in an effort to break into these computers. The effort to break in failed, but the user's automatic dialing mechanism made repeated use of the network company's communications service. In turn, the network company billed the host company for the time during which the unauthorized user had accessed its communications line. This

is obviously unfair to the host company. Where billings to a host company for incidents such as this exceed $1,000 in a one-year period, the Committee believes they should be subject to prosecution under this subsection.

Similarly, the Committee is concerned that authorized users of computer services might incur substantial costs as a result of relying on information contained in a database that has been tampered with. For example, an individual who invests in a stock, after having read a computerized market analysis that had been altered to make it appear the stock's potential had improved, has clearly incurred a cost. The Committee intends that those costs also be permitted to count toward the $1,000 valuation.

The second circumstance in which this subsection will penalize alteration, damage, or destruction is in connection with data relating to medical care and treatment. The Sloan-Kettering case discussed earlier in this report is but one example of computer crimes directed at altering medical treatment records. Where such conduct impairs or potentially impairs an individual's medical care, the Committee does not believe a showing of $1,000 in financial losses is necessary. Tampering with computerized medical treatment records, especially given the potentially life-threatening nature of such conduct, is serious enough to warrant punishment without a showing of pecuniary loss to the victim or victims. The Committee also wishes to make clear that convictions are attainable under this subsection without a showing that the victim was actually given an incorrect or harmful treatment, or otherwise suffered as a result of the changed medical record. That his examination, diagnosis, treatment, or care was potentially changed or impaired is sufficient to warrant prosecution under this subsection.

Two other important concerns have also been expressed to the Committee regarding the reach of the new subsection (a)(5). The first is that it might cover authorized "repairs" to a computer system because "alteration" of the data is part of the gravamen of the offense, and repairs presumably can involve altering data. It is not the Committee's intent to criminalize properly authorized repair activities. For example, this section does not prohibit employees of communications common carriers from engaging in activities that are necessary to the repair of the carrier's service. The Committee believes that the requirement in subsection (a)(5) that alterations occur after an unauthorized access is sufficient in itself to preclude its application to authorized repairs but wishes to leave no doubt that authorized repair activities are not covered by (a)(5).

The second concern is that (a)(5) might be construed as criminalizing the use in computer leasing services of automatic termination devices or so-called "time bombs". Frequently, a provider of computer services will build into his program a mechanism that automatically terminates the service if a user fails to pay his bill for the service on time. Concerns have been expressed that the provider might be considered liable under (a)(5) for having "prevented authorized use" of the service. That is not the Committee's intent. Having failed to pay his bill for the Committee service, the delinquent user is no longer an "authorized user" of the service, and termination of his access to the service is not an offense under this subsection.

The new subsection 1030(a)(6) to be created by the bill is a misdemeanor offense aimed at penalizing conduct associated with "pirate bulletin boards," where passwords are displayed that permit unauthorized access to others' computers. It will authorize prosecution of those who, knowingly and with intent to defraud, traffic in such computer passwords. If those elements are present—and if the password in question would enable unauthorized access to a Federal Government computer, or if the trafficking affects interstate or foreign commerce—this subsection may be invoked. The concept of "traffic" means to transfer, or otherwise dispose of, to another, or to obtain control of with intent to transfer or dispose of such passwords; the concept was borrowed from 18 U.S.C. 1029 relating to credit card offenses. The Committee also wishes to make clear that "password", as used in this subsection, does not mean only a single word that enables one to access a computer. The Committee recognizes that a "password" may actually be comprised of a set of instructions or directions for gaining access to a computer and intends that the word "password" be construed broadly enough to encompass both single words and longer more detailed explanations on how to access others' computers.

Section 2(e) eliminates the specific conspiracy offense in the present law. The Committee intends that such conduct be governed by the general conspiracy offense in 18 U.S.C. 371.

Section 2(f) conforms the "fine" provisions of 18 U.S.C. 1030 and this bill with the general fine provisions of the Criminal Fine Enforcement Act of 1984. It also contains the penalty provisions for the two new felony provisions (5 years first offense, 10 years second offense) and one new misdemeanor/felony provision (one year first offense, 10 years second offense).

Section (2)(g) establishes definitions for a "Federal interest computer," "State", "financial institution", "financial record", the term "exceeds authorized access," and the term "department of the United States", all of which are self-explanatory. The only committee note is that obtaining information as encompassed in the definition for "exceeds authorized access" would include observing information as we discussed under Section 2(a)(2) supra.

Section 2(h) conforms the exception for proper law enforcement and intelligence activity in the computer crime bill with the credit card legislation in 18 U.S.C. 1029(f).

Finally, the Committee wishes to make two general observations that apply to each of the computer crime offenses amended or created by S. 2281.

First, the Committee recognizes the necessity that computerized information be considered "property" for purposes of Federal criminal law. To date, computer users and providers of computer services have had to wrestle with a criminal justice system that in many respects is ill-equipped to handle their needs. Computer technology simply does not fit some of the older, more traditional legal approaches to theft or abuse of property. For example, computer data may be "stolen" in the sense that it is copied by an unauthorized user, even though the original data has not been removed or altered in any way. As long ago as 1983, the Department of Justice stated that:

> Any enforcement action in response to criminal conduct indirectly or directly related to computers must rely upon a statutory restriction dealing with some other offense. This requires the law enforcement officer, initially the agent, and then the prosecutor, to attempt to create a "theory of prosecution" that somehow fits what may be the square peg of computer fraud into the round hole of theft, embezzlement or even the illegal conversion of trade secrets.[13]

These enforcement problems can largely be overcome by recognizing computerized information as property. The Congress began that recognition by enacting the Computer Fraud and Abuse Act of 1984. The Committee intends S. 2281 to affirm the government's recognition of computerized information as property.

Secondly, the Committee wishes to make clear its intent to distinguish between conduct that is completely inadvertent and conduct that is initially inadvertent but later becomes an intentional crime. It has been suggested that this is a difficult line to draw in the area of computer technology because of the possibility of mistakenly accessing another's computer files. Nevertheless, the Committee would expect one whose access to another's computer files or data was truly mistaken to withdraw immediately from such access. If he does not and instead deliberately maintains unauthorized access after a non-intentional initial contact, then the Committee believes prosecution is warranted. The individual's intent may have been formed after his initial, inadvertent access. But his is an intentional crime nonetheless, and the Committee does not wish to preclude prosecution in such instances.

IV. Agency Views

In its testimony on April 16, 1986, the Department of Justice supported S. 2281, although it recommended several amendments to the bill.[14] The Committee adopted some of those recommendations, including an amendment clarifying the degree to which the offense in subsection 1030(a)(3) must affect the operation of the Government computer in question. Many of the Department's recommendations were incorporated into the Committee's report on S. 2281.

V. Congressional Budget Office Statement

U.S. Congress,
Congressional Budget Office,
Washington, DC, June 25, 1986.

Hon. Strom Thurmond,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has reviewed S. 2281, the Computer Fraud and Abuse Act of 1986, as or-

[13] Statement by John C. Keeney, Deputy Assistant Attorney General, Criminal Division; before the Senate Subcommittee on Oversight of Government Management, Committee on Governmental Affairs; October 26, 1983.

[14] See, Statement of Victoria Toensing, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, before the Senate Judiciary Committee; April 16, 1986.

dered reported by the Senate Committee on the Judiciary, June 12, 1986. We estimate that no significant cost to the Federal Government, and no cost to State or local governments would result from enactment of this bill.

S. 2281 makes a number of amendments to Section 1030 of Title 18 of the United States Code, dealing with computer fraud and related activity. These amendments include several changes in the standards determining violations of the law. The bill extends the existing Federal privacy protection of computerized financial information to cover all such records of financial institutions, as defined in the bill, and clarifies the prohibition against unauthorized access of computers used by the U.S. government. S. 2281 also creates three new offenses involving theft in the form of unauthorized computer access with the intent to defraud, malicious damage through unauthorized computer access, and trafficking in computer passwords with the intent to defraud. The provisions governing fines for new and existing offenses would be made to conform with the Criminal Fine Enforcement Act of 1984.

Based on information from the Department of Justice, we expect that S. 2281 would provide a more specific statute on which to base the investigation and prosecution of these activities, which the Department is currently undertaking under other authority. Enactment of the bill is not expected to result in a significant change in the government's law enforcement practices or expenditures.

If you wish further details on this estimate, we will be pleased to provide them.

With best wishes,

Sincerely,

RUDOLPH G. PENNER.

VI. REGULATORY IMPACT STATEMENT

Pursuant to paragraph 11(b), rule XXVI, of the Standing Rules of the Senate, the Committee has concluded that the bill will have no direct regulatory impact. The bill encourages, but does not require, the agencies and departments of the Federal Government to develop clear rules and sanctions regulating the use of Government computers by employees and other authorized individuals. The bill also encourages other owners and users of Federal interest computers to establish clear statements of the scope of authority for those who use the Federal interest computers.

VII. CHANGES IN EXISTING LAW

In compliance with paragraph (12) of rule XXVI of the Standing rules of the Senate, changes in existing law made by S. 2281 are as follows: Existing law proposed to be omitted is enclosed in black brackets, new material is printed in italic, existing law in which no change is proposed is shown in roman.

UNITED STATES CODE

* * * * * * *

TITLE 18: CRIMES AND CRIMINAL PROCEDURE

* * * * * * *

CHAPTER 47—FRAUD AND FALSE STATEMENTS

* * * * * * *

* * * * * * *

§ 1030. Fraud and related activity in connection with computers

(a) Whoever—

(1) knowingly accesses a computer without authorization [, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend] *or exceeds authorized access*, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;

(2) [knowingly] *intentionally* accesses a computer without authorization [, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend] *or exceeds authorized access*, and thereby obtains information contained in a financial record of a financial institution, [as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.),] or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or

(3) [knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation;] *intentionally, without authorization to access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects the use of the Government's operation of such computer;*

(4) Knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;

(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby—

(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

* * * * * *

(b)[1] Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

[(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not great than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both.]

(c) The punishment for an offense under subsection (a) or (b)(1) of this section is—

(1)(A) a fine [of not more than the greater $10,000 or twice the value obtained by the offense] *under this title* or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine [of not more than the greater of $100,000 or twice the value obtained by the offense] *under this title* or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(2)(A) a fine [of not more than the greater of $5,000 or twice the value obtained or loss created by the offense] *under this title* or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2) [or (a)(3)], *(a)(3) or (a)(6)* of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine [of not more than the greater of $10,000 or twice the value obtained or loss created by the offense] *under this title* or imprisonment for [not than] *not more than* ten years, or both, in the case of an offense under subsection (a)(2) [or (a)(3)], *(a)(3) or (a)(6)* of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph[.]; *and*

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph.

* * * * * * *

(e) As used in this [section,] *section—*

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device[.];

(2) the term "Federal interest computer" means a computer—

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or

(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States;

(4) the term "financial institution" means—

(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

(D) a credit union with accounts insured by the National Credit Union Administration;

(E) a member of the Federal home loan bank system and any home loan bank; and

(F) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter; and

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

VIII. ADDITIONAL VIEWS OF MESSRS. MATHIAS AND LEAHY

We are pleased to join with our colleagues on the Judiciary Committee in reporting S. 2281, the Computer Fraud and Abuse Act of 1986. The authors of the legislation have effectively carried out a delicate and complex task. The result is a bill that offers an appropriate Federal response to the real and growing problem of computer crime.

The committee's report on S. 2281 thoroughly describes the scope of that problem, and the details of that response. As the report notes, this bill builds upon the computer crime legislation enacted in the closing days of the 98th Congress. We wish to emphasize that S. 2281 not only refines and extends the computer crime provisions of Public Law 98-473, it also refocuses that legislation on its principal objectives, and minimizes the likelihood that it will be misused to cut back on the American public's right to know about the activities of its government.

As enacted in 1984, the provision now codified as section 1030(a)(3) of title 18 makes it a crime to "knowingly use . . . or disclose information in [any] computer . . . operated for or on behalf of the Government of the United States," when the defendant gains access to the computer without authorization or his conduct exceeds the scope of his authorization. By its literal terms, this provision sweeps in all computerized government information, including documents that must, under the Freedom of Information Act, be disclosed to any member of the public upon proper request. Section 1030(a)(3) also glosses over the reality that the existence or exact scope of a government employee's authority to access a particular computerized data base is not always free from doubt. Under these circumstances, any employee asked to release data that must be disclosed under the FOIA would be understandably reluctant to do so unless assured of the precise contours of his authorization to access it. An incorrect assertion of authorization could expose the employee to prosecution and imprisonment. Any prudent employee would resolve doubts against disclosure, a conclusion directly contrary to the principles of open government underlying the FOIA.

Motivated by these concerns arising from provisions of the House-passed computer crime bill, the Senate, on the next-to-last day of the 98th Congress, unanimously approved our amendment to the bill which narrowed the sweeping provisions of the disclosure offense under section 1030(a)(3). Unfortunately, in the rush toward adjournment, the House never acted on the Senate amendment to this bill. Instead, the free-standing computer crime legislation was overtaken by a continuing appropriations resolution, to which had been appended hundreds of pages of crime legislation, including portions of the unamended House computer crime bill. Thus, in a particularly graphic lesson in the shortcomings of legislation by

rider, section 1030(a)(3) was signed into law, despite the Senate's unanimous view that its scope was too broad.

The bill we now report, unlike its predecessor, has had the benefit of nearly 2 years of careful scrutiny and study by the Subcommittee on Criminal Law. Among the many improvements that it would make is a complete revision of section 1030(a)(3). The revised provision includes three salutary features that minimize the possibility that this computer crime legislation could be misused to weaken the Freedom of Information Act, or to impose unnecessary obstacles to the public's right to know about government activities.

First, the mental state required to establish a violation of revised section 1030(a)(3) is increased from "knowingly" to "intentionally." As the committee report points out, the "intentional" standard precludes criminal liability for inadvertent acts of unauthorized access. Instead, it is "designed to focus Federal criminal prosecutions on those who evince a clear intent to enter, without proper authorization, computer files or data belonging to another."

Second, S. 2281 would eliminate coverage for authorized access that aims at "purposes to which such authorization does not extend." This removes from the sweep of the statute one of the murkier grounds of liability, under which a Federal employee's access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization. As the committee report points out, administrative sanctions should ordinarily be adequate to deal with real abuses of authorized access to Federal computers (assuming, of course, that no other provision of section 1030 is violated). Like the heightened scienter requirement, this change serves to minimize the likelihood that a Federal employee, uncertain about the scope of his authority, would face a Hobson's choice between the disclosure mandates of FOIA and the criminal sanctions of title 18.

Finally, revised section 1030(a)(3) would not apply to access by a Federal employee of computers of that employee's own agency. This exclusion recognizes the reality that computer access rules for employees within a single agency are rarely as clear as rules governing access by outsiders to that agency's computers. Revised section 1030(a)(3) would provide prosecutors a clear, workable rule, regardless of the intricacies of a particular agency's computer access policies: absent a fraudulent motive, an employee could not be prosecuted for simple "trespass" into one of his agency's own computers.

Like any bright-line rule, this one does not conform perfectly to the behavior it addresses. To treat employees of other agencies as "outsiders" for the purposes of this statute may, in an exceptional instance, work some hardship. The committee report notes that the revised subsection may, on rare occasions, prove underinclusive; as well, it may be overinclusive in unusual cases. The fact is that many Federal agency data bases are separated from those of sister agencies not by well-defined walls, but by permeable membranes. Information sharing may become computer sharing without formal protocols of authorization. Access by one who appears to be an "outsider" to the agency may be not only excusable, but helpful to the agency's mission.

But certainly this imprecision can be accommodated. Just as other criminal sanctions may well be at hand in cases that fall through the net of the revised subsection (a)(3), so administrative sanctions—and, of course, the discretion not to prosecute—will remain available for those cases of interdepartmental unauthorized access that do not justify prosecution.

S. 2281's revisions to section 1030(a)(3) do not track the approach adopted by the Senate in 1984, and embodied in our bill in this Congress, S. 610, for correcting the course set by the 1984 computer crime legislation. Both the 1984 Senate amendment, and S. 610, focused on the disclosure aspect of the offense created by section 1030(a)(3), and sought to exclude from the offense information whose disclosure ought not to be discouraged. Because the revised subsection is a simple trespass offense, rather than one requiring disclosure or some other act beyond access to the data, our earlier approach to the problem is now less apposite. We think the balance struck by S. 2281 on this issue is reasonable. It largely ameliorates our concern about the effect of section 1030(a)(3) on the free flow of government information to the American people. It goes far toward restoring the incentive for Federal employees to comply voluntarily with the Freedom of Information Act in their dealings with requests for computerized government information. At the same time, it gives the Government an adequate prosecutorial tool for deterring and punishing unauthorized access to sensitive Government information by those who have no colorable claim of a right to obtain it outside proper channels.

In this and other aspects, S. 2281 constitutes a real improvement on existing computer crime law. The Subcommittee on Criminal Law, under Senator Laxalt's leadership, and its House counterpart, the Subcommittee on Crime, have crafted well-considered and constructive legislation, and we are pleased to support it.

○